# NASA Procedural Requirements

**COMPLIANCE IS MANDATORY**

**NPR 8705.2A**
Effective Date: February 07, 2005
Expiration Date: February 07, 2010

Printable Format (PDF)

## Subject: Human-Rating Requirements for Space Systems

**Responsible Office: Office of Safety and Mission Assurance**



# Appendix C. History and Rationale

## C.1 Human-Rating Requirements

C.1.1 This appendix is included to provide a history and rationale to enhance the understanding of the human-rating requirements. This section does not negate application of requirements to a system or alter the requirements in NPR 8705.2. If it is interpreted to be in conflict with the requirements, the requirements supersede this appendix.

## C.2 Introduction to Human Rating

C.2.1 The human-rating process for NASA programs has not fundamentally changed since the Mercury program. This process is meant to ensure the incorporation of design features and requirements necessary to maximize the health and safety of the human participants. This process demands that system safety be embraced at all levels of the program. It demands rigorous design, development, and testing as well as meticulous verification and process control. It dictates stringent management oversight and accountability of all participants. This process culminates in a formal certification for operational readiness and continues through the life of the program.

C.2.2. Human-rating requirements fall into two basic categories, Management and Design/Engineering/Implementation (Table C-1). Management rigor is required to ensure emphasis on crewed flight awareness, the development of a robust engineering and management review process, complete and timely problem reporting and corrective action, process controls for documentation, configuration, and certification, and finally, the utilization of appropriate and accurate risk analysis tools. Engineering requirements are aimed at the application of conservative design methods and standard practices, developing redundancy in critical systems, utilizing proven technology, and verification of design through extensive test and analysis.

## C.3 Applicability of Requirements

C.3.1 Human-rating requirements are applicable to any system which transports or houses humans or interfaces with other systems which transport or house humans. Therefore, many uncrewed elements may also be subject to these requirements. For example, currently the expendable launch vehicle is not used in concert with a human-rated system, and so these requirements do not apply. However, if an expendable launch vehicle is used as part of a crewed launch system, human-rating requirements apply.

C.3.2 Human-rating requirements are to be reviewed carefully to ensure that requirements which do not apply (e.g., ascent abort requirements do not apply to surface rovers) are culled out of the initial requirements set via the tailoring process. The tailoring process is not intended to accommodate the deletion of requirements which are costly, technically difficult, or create a longer schedule. The process is strictly for requirements which are not applicable to a specific system.

C.3.3 Exceptions are to be utilized when a requirement is not applicable to some subsystems, such as requirements for two-failure tolerance on primary structure, but is generically applicable to other subsystems. If the program has an approved Human-Rating Plan and then determines that it cannot meet a planned human-rating requirement for a subsystem (e.g., structures), and this variance is permanent (e.g., the system will not be designed to meet the requirement), the program is able to request an exception. If the exception is approved, the program updates the

Human-Rating Plan to reflect this.

C.3.4 All other variances from requirements are handled through the waiver and deviation process to ensure appropriate visibility into the inability to meet requirements.

## C.4 The Human-Rating Plan

C.4.1 The Human-Rating Plan documents how the program plans to comply with the human-rating requirements throughout the system's life cycle. The plan is, by necessity, a living document, or a multiple volume set, in order to comply with the content and approval requirements of this document. The plan need not be a stand-alone plan. As a matter of fact, it may be more expedient to fold it into overall systems plans and requirements; however, it is essential that the human-rating requirements are easily identified and extractable from these systems level documents, so as to be able to meet human-rating requirement review milestones. Most important is not where the requirements reside, but that there be clear identification of specific human-rating requirements and clear traceability from requirements to demonstration of compliance.

Table C-1: Areas of Emphasis for Human Rating

| | |
|---|---|
| Fundamental Tenants of Human Rating Management: | • Continuous Attention to Human-Rating Throughout the Program<br>• Human Health and Safety Priority<br>• Design/Engineering/Implementation:<br>• Well Established and Proven Aerospace Design Standards and Analytical Approaches<br>• Conservative Design Factors<br>• State-of-the-Art Technology<br>• High Quality<br>• Comprehensive Ground Test and Flight Test Before Crewed Flight<br>• Crew Survival Modes<br>• Two-Failure Tolerance to Prevent Fatality or Permanent Disability<br>• Hazard Detection and Safeing<br>• High Reliability Parts and Components<br>• Well Understood and Characterized Materials |

## C.5 Management Requirements

C.5.1 Program management is crucial to the success of human space flight and requires active involvement in every phase of the program. Proper attention by program management begins in the early formulation of the program by applying the requirements in this document and implementing them throughout the life of the program. It is ultimately the program manager's responsibility to assure the successful implementation of all human-rating requirements.

C.5.2 An endeavor as complex as human space flight requires that continuous attention be paid to all aspects of human rating throughout the life cycle of the program. Systems engineering, safety processes, risk management, certification, and sustaining engineering all require direct management involvement to assure the safety of the space flight system and its crew.

## C.6 Technical Requirements

C.6.1 The technical requirements specified in this document are based on a history of successful space flight

experience, as well as some difficult lessons learned. Space systems operate in an inherently high-risk environment, especially during the ascent and descent phases, and only the best practices of the aerospace industry are sufficient to give reasonable assurance that a failure does not result in a crew or passenger fatality or permanent disability.

C.6.2 Design and Test

C.6.2.1 Emphasis during design is on using established aerospace design standards, since these standards are based on lessons learned regarding the design and operation of space flight systems. While space flight systems design is built upon decades of aircraft experience, the unique operations and environments of the space flight missions lead to a different and even more stringent set of design requirements. It is essential that the design of a human-rated space flight system fully account for these differences. Historically, human rating was accomplished through the use of aircraft safety factors instead of the lower safety factors typical of uncrewed military launch vehicles, eliminating single failure points, and providing crew and passenger survival systems in case of a catastrophic vehicle failure. Incorporating historical and evolving lessons learned is critical to ensuring the highest level of design safety. As the design evolves, all system trades are focused on ensuring the integrity of the system design to meet human-rating requirements. The detailed design requirements and practices specified in JSCM 8080.5 represent significant crewed spacecraft design and operational knowledge applicable to a wide range of crewed space flight activities, and are to be utilized in all spacecraft and ground systems design.

C.6.2.2 The human-rated space flight system is designed, built, inspected, tested, and certified specifically addressing the requirements for human rating from the early formulation of the program. In addition to system and subsystem testing to ensure that design requirements are achieved, components are qualification and acceptance tested to ensure that adequate design margin exists at the component level for vibration, acoustic, thermal, shock (including pyrotechnic shock), and pressure/aerodynamic/structural loads, and to ensure the production hardware meets the quality of the certification hardware. Military Standard 1540, Test Requirements for Launch, Upper-Stage and Space Vehicles, dated September 1994, or equivalent component qualification and acceptance testing standards are good guidelines for the development of testing requirements. The use of dedicated qualification components is recommended. Flight components are acceptance tested in the previously noted environments, as applicable, to ensure that each individual component has adequate performance margin for its intended use. Policies for required margins for each environment for qualification and acceptance are developed by the program. The performance margins are based on NASA and Military Standards, as well as successful similar programs.

C.6.2.3 For systems requiring incremental assembly where elements involve distributed end-to-end subsystems in low Earth orbit or beyond Earth orbit, it is prudent to conduct multiple-element integrated testing prior to launch. Use of approaches such as testing elements in logical groupings with appropriate fidelity emulations of interfaces is acceptable. The use of emulators is, however, less desirable than testing the actual hardware, and additional care needs to be exercised in the development of interface controls to ensure the emulators reflect the true "as built" configuration of the system. Testing is carried out with software possessing flight functionality and flight hardware in flight configuration. Priority is given to interface validations of hardware and hardware/software interaction. If applicable, end-to-end testing of command and telemetry links between the control center(s) and the vehicle can be accomplished.

C.6.3 Flight Test

C.6.3.1 No space flight system can be certified on the basis of analysis alone; therefore, comprehensive flight test is a very important part of the certification process. These flight tests can be done with humans providing all practical testing and analysis is completed and the vehicle is "Certified."7 Flight experience has shown that many critical performance parameters are highly design-specific and require thorough operational test and checkout to verify. Virtually all flight programs have shown important areas where flight and operational experience did not match the predictions. The design process for space flight systems is based on analyses and simulations that are highly dependent upon the analytical math models of the flight environment and the space flight systems hardware. Current and expected technologies require that many of these math models be based on estimates, approximations, and simplifications of the real world.

C.6.3.2 Whenever possible, it is good practice to conduct the flight test program across the entire mission profile. A sufficient number of flights are needed so that the flight test data validates the analytical math models in order to predict the performance of the space flight systems at the edges of the operational envelopes. This is generally possible for systems with discrete mission profiles of manageable duration such as Earth-to-orbit and crew rescue space flight systems. These systems can usually be operated through several complete ascents, orbital transfers, and/or descent profiles and can give good confidence in the suitability of the design for the planned mission. For some systems, a flight test across the entire mission profile may not be feasible, either due to the excessive amount of time required to cover the planned mission duration, or the lack of suitable conditions to test, as in the case of planetary landing space flight systems. In these cases, a series of tests encompassing all elements of the mission profile under actual or high-fidelity simulated conditions is the best method for demonstrating capability. Limited testing backed with extensive analysis and simulation may be an acceptable substitute for well-understood environments. Flight testing requirements apply to extravehicular mobility units or other systems, including those that have a self-contained propulsion system.

C.6.4 Human Engineering and Life Support

C.6.4.1 NASA has developed life support systems requirements that encompass all habitable space environments inclusive of the preflight, in-flight, and post-flight phases. An environment suitable for human habitation has been defined for pressurized elements according to the specifications and standards in NASA STD 3000. Human-factor-compliant designs and monitoring of critical environmental health parameters are necessary for optimal human performance. JSC 26882, NASA Space Flight Health Requirements, also discuss crew habitability and life support systems. These standards also apply to uninhabited space flight systems volumes that may require ingress and egress by a crewmember or passenger in flight such as a pressurized logistics mission cargo carrier. These requirements have evolved from NASA's Mercury, Gemini, Apollo, Skylab, Shuttle Transportation System, the International Space Station, and multiple extravehicular suited programs. Long-duration space flight requirements are derived from NASA's Lunar, Skylab, Extended Duration Orbiter, International Space Station, and Phase One Mir life sciences programs. Other important human engineering standards to be relied upon are MIL STD 1472, DOD Design Criteria Standard - Human Engineering, and NASA/TM-2002-210785, Guidelines and Capabilities for Designing Human Missions.

C.6.5 Software

C.6.5.1 Providing effective safety of a space flight system dictates that controls be established for computer-based control systems. A computer-based control system utilizes computer hardware, software, and/or firmware to accept input information and processes that information to provide outputs to a defined task. Specific requirements for computer-based control of systems address the following: computer-based control system software requirements applied regardless of function; requirements for the control of functions that must work; and requirements for functions whose inadvertent operation would cause a hazard (such as must-not-work functions). An example reference for these technical requirements is SSP 50038, Computer-Based Control System Safety Requirements, International Space Station program.

C.6.5.2 Confirming integrity of software design and testing is essential to human space flight systems, and requires the use of independent software verification and validation to ensure that the software requirements are consistent and complete, that the scope of the test matrix covers all requirements, and that all discrepancies in the test results are resolved before flight. Software has become a key component in the safety and reliability of today's aerospace space flight systems, consequently all critical software is expected to be tested to the same levels of quality as the hardware systems. Critical software is any software component whose failure or unanticipated performance could lead to the crew or passenger fatality or permanent disability. This includes the flight software as well as ground software that can affect human health and safety.

C.6.6 General Aerospace Standards and Lessons Learned

C.6.6.1 Program and project managers are encouraged to access and use the NASA Headquarters Office of the Chief Engineer Web site which includes links to standards-developing organizations as well as links to lessons learned and best practices for aerospace design. Additional information on traditionally accepted design and verification methods and standards can be obtained through historical certification requirements documents listed in Appendix A of this document. The intent of the detailed design requirements and practices specified in these documents is to be incorporated in the design of human-rated space flight systems.

C.6.7 Two-Failure/Two-Inadvertent Action and Error Tolerant Design Requirements

C.6.7.1 As defined "fault (failure) tolerance" is the ability of a system or subsystem to perform its function(s) or (in case of a safety system) maintain control of a hazard in the presence of failures of its components.

C.6.7.2 Here, a component is defined as an individual constitutive element of the system. Components include passive hardware (such as pipes, wires, vessels, etc.), active hardware (such as pumps, values, actuators, relays, etc), firmware (computer programs and data loaded into a class of memory that cannot be dynamically modified by the computer during processing), software (computer programs and data that can be dynamically modified during processing), and humans. All systems (and subsystems) are made up of components, whether passive or active.

C.6.7.3 The analysis of failures involves understanding the component's function and evaluating both the context (environment, operating conditions, state of the remainder of the system) within which the component is called upon to function and its modes of failure. For example, the evaluation of passive components considers their passive functions and both their external and internal environments (microgravity, temperature, ionizing atmospheres, etc.) along with their failure modes (i.e., leaks in pipes or pressure vessels or minor bleed off shorts in wiring; catastrophic ruptures accompanied with shrapnel or complete dead shorts with sparks and heat). Analyses of active components involve the same process of considering their function, the context in which they are called upon to operate, and their failures modes.

C.6.7.4 Analysis of failures includes human failures or errors. An error, in this context, pertains to the failure of the human component. In almost all systems, the most complex component is the human. In addition, humans are considered active components where some human actions are learned rote responses to input stimulus while other actions are a result of cognitive processes. The human component also has the capacity to "fix" or "repair" its errors.

Basically, a human error can be classified as an error of commission (performing the wrong action) or omission (failing to perform an action). When analyzing human errors, the same process used to analyze failures is employed. The analysis considers the action to be performed, the context (environment, performance shaping factors, operating conditions, state of the remainder of the system) within which the human is called upon to perform the action, and the modes of failure. To some degree, the analyses of software components are similar to the analyses of human components. This methodology has been used to analyze countless error in aerospace and other industries and can be performed with commercially available software.

C.6.7.5 In the perspective of the human-rating requirements, the two-failure tolerance and two-inadvertent action requirements are levied in the design of space systems only to the extent that they prevent or reduce the possibility of permanent disability or loss of life to the crew and space system passengers.

C.6.7.6 Therefore, two-failure/two-inadvertent action is the ability of the system or subsystem to perform its function(s) or (in case of a safety system) maintain control of a hazard in the presence of two failures/two inadvertent actions of its components. Said another way, it is a requirement that the space system be designed to tolerate two component failures/inadvertent actions without resulting in permanent disability or loss of life.

C.6.7.7 Appropriate failure tolerance is a fundamental aspect of human rating. Failure tolerance is a term frequently used to describe minimum acceptable redundancy, but it may also be used to describe two similar systems, dissimilar systems, cross-strapping, or functional interrelationships that ensure minimally acceptable system performance despite failures. It is highly desirable that the space flight system performance degrades in a predictable fashion that allows sufficient time for failure detection and, when possible, system recovery even when experiencing multiple failures. This is true for failures involving hardware, software, and humans.

C.6.7.8 Due to the demands of a long duration mission, failures in systems will occur. Therefore, long duration mission design may use maintenance and system reconfiguration to restore failed functions and sustain two-failure tolerance and meet the two-inadvertent action requirement.

C.6.7.9 Once potential failures/errors are identified, system design trades can be made to prevent the failures or mitigate their effects. For example, system design may incorporate dissimilar systems performing the same function, cross strapping, failure tolerance, failure detection, and failure recovery capabilities to minimize the negative consequences of failures. Space flight system hardware is designed for inherent reliability at the component level, but the architecture of the system also needs to protect against random failures and minimize the probability of crew or passenger fatality or permanent disability. In systems with relatively short periods of operation, or where dynamic flight modes (such as powered ascent) are involved, installed redundancy is the principal means of ensuring the system's reliability. In space flight systems with longer missions and more time for recovery from failures, maintenance and logistics resupply are critical. Elements that are designed for minimum risk, such as primary structure and thermal protection systems, are generally exempt from two failure tolerance requirements.

C.6.7.10 In practice, not all human errors can be identified, nor can systems be designed to prevent all human errors in operational contexts. However, many errors can be prevented, the frequency of human error can be minimized through design, and when error prevention is not possible, design features can be put in place to detect and correct the errors and mitigate the negative consequences.

C.6.7.11 When error prevention is not technically feasible or increases overall system risk, error can be managed through designs that assist the human in detection of the error and provide controls and time to recover from the error.

C.6.7.12 Human factors engineering uses these concepts along with detailed knowledge of human anthropometrics (ergonomics), cognitive reasoning in light of stimuli, rote memory, training, experience, feedback, sensory perception (sight, sound, olfactory, tactile) and the effects of environmental inputs (performance shaping factors) to design systems that interface with and are controlled by the human component. Meeting the two-failure tolerance/two-inadvertent action requirements is essential to operational safety where systems and subsystems are designed with full consideration of the actions of the human component in conjunction with potential failures of hardware, firmware, and software, the environments under which these actions are performed, and the potential human failures modes. This requirement also provides the designer a lot of flexibility establishing when a given error is impracticable or technically not feasible to eliminate.

C.6.8 Common Cause Failures

C.6.8.1 When using redundancy to meet the two-failure tolerance/two-inadvertent action requirements, it is a "best practice" to eliminate common cause failures/inadvertent actions and/or mitigate the risk. These types of failures /inadvertent action occur when both redundant systems fail because of some common reason, for example, the use identical components, exposure to common adverse environments, common incorrect maintenance operations, and components called upon to function outside their specifications. A method for reducing the potential for common cause failures would be to use dissimilar systems performing the same function.

## C.7 Human Interfaces and Intervention

C.7.1 Industry experience does not support placing humans on board without the capability to intervene in the case of malfunction or other unanticipated events. History has shown that the overall contribution of the crew increases mission reliability since, in addition to being available to respond to hardware failures and unanticipated natural events, a human can overcome many latent errors in hardware and software design given the opportunity and if proper attention is paid to the human-machine interface. The contribution of the crew is maximized when it is provided with the proper insight, intervention capability, control over vehicle automation, authority to enable irreversible actions, and autonomy from the ground.

C.7.2 The intent of human interface requirements is that the system be designed to provide the operators with the required level of insight, feedback, and control appropriate to the flight phase, system and function:

a. Feedback for human commands is a system communication that directly results from the user's input to the system and provides the user with information that allows him/her to determine if the input was received and what has been accomplished. Determining the appropriate level of crew control over individual functions is a decision that is made separately for specific vehicles.
b. Per the human-rating requirements, the system is designed so that the crew has control of the configuration and operation of all functions that can affect safety of flight. Specifically, if a valve or relay can be controlled by a computer, then that same control ought to be offered to the crew where the crew can be a viable part of the system design and perform that function. For example, it is not practical for a crew member to have control of individual valves that meter the flow of propellant to the engines, but a human interface capability (e.g. throttle) which incorporates multiple valve movements to achieve a desired end state (reduce or increase thrust) could be incorporated into the design to meet requirements.
c. Per the human-rating requirements, the system is designed so that the crew has control over those systems that directly affect the performance of the crew such as cabin temperature, cabin exterior/interior lighting, and radio volume within safe operating limits, so that, within the capabilities of the subsystem, crew performance can be optimized. (Safe limits as defined by the Occupational Health and Safety Administration - for example, it is possible to adjust radio volume to a level that may cause hearing damage or impairment.)

## C.8 Crew Stations and Displays

C.8.1 It is a best practice to apply attention to the human-system interface to maximize insight and minimize flight crew workload and errors. This holistic approach to designing the human-machine interface, including displays and controls, is required throughout the design process and, for each task identified, comply with applicable standards such as MIL-HDBK-1797. It is good practice in the design of the crew and machine interface to include iterative prototyping and usability evaluations with direct crew involvement.

C.8.2 The technology of displays and controls design continues to change and the state of the art can be applied to the human interface to minimize crew workload and errors. For example, the displays may be organized in a hierarchical fashion such that the highest level display provides an overview, the "big picture," with the provision for the crew to directly access additional displays for more specific details about the individual subsystems.

C.8.3 Specific designs for crew station configuration is dependent upon specific mission objectives and requirements. While the majority of space missions may be capable of being operated by a single, fully trained pilot, certain space missions may require more than one trained pilot due to increased workload. Vehicle designs that provide multiple functional crew stations can provide flexibility, improve safety, and enhance mission success. Multiple functional crew stations also provide redundancy for loss of displays or vehicle control devices.

C.8.4 Mockups and simulators can be developed to fully test the human-machine system in an operationally relevant context. A high-fidelity simulator is especially valuable for testing system performance in failure scenarios that cannot be safely tested with hardware and/or flight test. The human-in-the-loop functions ought to be evaluated under realistic scenarios, both nominal and off-nominal, to ensure they support the safety and reliability requirements of this document.

## C.9 Crew Workload and System Handling Requirements

C.9.1 The performance of the crew-vehicle interface can be measured in terms of workload, performance, and errors. It is good practice to develop crew and vehicle interfaces following accepted methods and standard practices, including concept development, rapid prototyping, and structured usability testing with flight crew involvement. The Bedford Workload Scale (Roscoe, 1984) or the Modified Cooper-Harper Scale (Casali & Wierwille, 1983) measure workload and may provide an estimate of how much workload margin is left over to perform additional tasks. The workload ought to meet the human-rating requirements even for off-nominal situations. Mission tasks cannot be scheduled at a pace that results in the degradation of crew performance. This is not intended to discourage a high-tempo of operations, but to result in the considerations of all factors that can adversely impact crew and therefore system performance.

C.9.2 To maximize flight crew performance in areas where vehicle maneuvering is required, the spacecraft is to exhibit Level I control qualities as measured using the Cooper-Harper Rating Scale (NASA TND-5153). Level I handling qualities ought to be available in all nominal phases of flight and most off-nominal situations. However, certain failures which degrade flight control surfaces or engine gimbaling may result in handling characteristics which are worse than Level I.

## C.10 Crew and Passenger Survival

C.10.1 Probability of Survival Requirements

C.10.1.1 Expectations for overall probability of crew and passenger survival are to be defined early in the program. This allows for allocation of risk to specific systems at the conceptual design phase, which is essential to guide the program management and engineer in design trades. Inclusion of reliability estimation and allocation during system definition facilitates timely and effective decision making before critical design solutions are precluded. It is well understood that crew survival systems are difficult to retrofit into a mature design; however, options for robust design and crew escape systems that increase the probability of crew and passenger survival are feasible if addressed in early mass allocations.

C.10.2 Crew and Passenger Survival Modes

C.10.2.1 Crew and passenger survival modes (such as, but not limited to, abort, escape, safe haven, emergency egress and rescue) are a significant design element of space systems given the relative immaturity of human space flight. The overarching objective of a crew and passenger survival centered design is for the system to withstand critical system failure with appropriate redundancy and robust design. The need for survival modes beyond this robust design is an acknowledgement that the space system cannot always be designed to anticipate and withstand all failure modes. A robust crew survival capability is necessary for any human rated system, but the specific determination of survival modes is highly dependant on the system configuration.

C.10.3 Abort vs. Escape

C.10.3.1 For ascent, abort is always the preferred mode of operation after failure. Exposure to the environment, addition of complex extraction systems, and limited capability for system verification all add risk for a successful crew or passenger extraction. It is good design practice for abort modes to remain within the performance envelope of the crew escape system to survive additional system failures or other problems during the abort trajectory.

C.10.3.2 Recovery from catastrophic failure modes during reentry necessitates robust design to withstand the event, to allow for landing with the failure, or to withstand the event and allow for subsequent escape and crew and passenger recovery. The ability to withstand significant failure through robust design and allow for a landing is always preferred over an escape. Robust design is defined as the implementation of design characteristics which provide resistance to catastrophic failure modes and tolerance to failure by supplying additional capability to withstand extreme off nominal circumstances and environments (e.g. structural hardening). Depending on system architecture, combinations of survival modes may be required to offset the uncertainty associated with verification of high probabilities of safe crew and passenger return.

C.10.3.3 A verified abort mode allows for crew and passenger return and crew recovery without exceeding the physiological and cognitive limits of the crew, while maintaining stability, control, structural, or thermal safety factors of the space flight system. Contingency abort modes, where stability, control, structural, or thermal safety factors are reduced, still retain positive margin and remain within physiological and cognitive limits of the crew. It is good practice to verify aborts with flight test.

C.10.3.4 Crew escape systems require extensive testing and analysis to verify the functional envelope and environment for system utilization, as well as detailed tests and assessments to ensure the system does not cause a fatality or permanent disability. Due to the dynamic and unpredictable nature warranting the use of crew escape systems, complete verification by integrated flight test is impossible. Crew escape systems may never be considered as a leg of redundancy.

C.10.4 Crew and Passenger Survival Risk Assessment

C.10.4.1 When determining the appropriate crew and passenger survival modes to employ for a given failure scenario, it is good practice to perform qualitative and quantitative risk analyses employing safety and reliability methodologies to determine the best solution for crew survival. Analyses of likelihood of success for candidate survival methods take into account the time required to successfully implement the method as compared to the time to effect of the hazardous situation. Variables such as exposure of the crew and passengers to the hazard in question (e.g., booster explosion), as might be the case for an escape, are analytically compared to the risks of attempting to execute a separation of the crewed spacecraft from the hazard. New hazards may be introduced by the employment of a given survival method (e.g., such as premature firing of an ejection seat) that are weighed against the potential risk mitigation gained from the method. Combined with detailed engineering analyses, these risk analyses provide a common yardstick to measure the potential for risk reduction or risk increase.

C.10.5 System Specific Implementation

C.10.5.1 Earth-to-Orbit

C.10.5.1.1 For some launch systems (i.e., capsule derivatives) 100 percent abort may be a viable option to meet requirements for crew and passenger survival; however, for other launch systems, escape modes may be required to achieve the desired probability of crew and passenger survival. The incorporation of survival modes on ascent is necessary, regardless of analytical risk assessments, due to the highly dynamic nature of the ascent flight regime and the increased likelihood of catastrophic, uncontainable failures.

C.10.5.2 Beyond Earth Orbit

C.10.5.2.1 Beyond Earth orbit missions require unique survival modes. Missions designed for beyond Earth orbit require sufficient power, consumables, and trajectory design to maximize crew and passenger survival capabilities. These modes include, but are not limited to: powered return, free return, pre-positioning capabilities, safe haven, and rescue. In general, the mission profile requires the space flight systems and their propulsion system to have sufficient propellant to fly off-nominal trajectories. The design can provide time for other systems or the crew to recover from a critical system failure. As a last resort, when abort modes are not feasible, a safe haven capability may be provided to ensure that survival capability and consumables exist to return the crew to a position from which a normal recovery or rescue can be conducted. It is good practice in long-duration mission planning to give consideration to pre-positioning consumables, spare parts, and other critical logistics and services to improve abort and safe haven capabilities.

C.10.5.2.2 Autonomy, functional redundancy, and tools to deal with the unexpected are a critical part of the design for safety. Technology will likely pace the schedule for accomplishing this.

C.10.5.3 Crew and Passenger Rescue

C.10.5.3.1 The crew and passenger rescue mission achieves its reliability through appropriate system design for availability, simplicity of hardware, and failure tolerance. Flight experience has shown that it is likely to be used at least once during the life of a Space System program, most likely due to a medical contingency. Since it may be attached to the Space System for extended periods of time and is essential to the Space System mission, operational availability on demand and high reliability throughout its on-orbit life are significant aspects of Space System design. To achieve acceptable levels of reliability and availability, on-orbit checkout and maintenance capabilities may be required.

C.10.5.3.2 Since crew rescue vehicles provide emergency escape, traditional abort and escape modes are not applicable. Consequently, the space flight system provides the capability to transport severely injured or ill crewmembers, in need of medical evacuation, safely to Earth.

C.10.5.4 Crew and Passenger Transfer

C.10.5.4.1 The main function of a crew transfer system is to ferry crewmembers and passengers to or from space flight systems. Since life support systems aboard a crew transfer vehicle may be limited, abort modes that allow for the safe recovery of crewmembers and passengers are critical.

C.10.5.4.2 When transferring crewmembers to or from space flight systems, there may be multiple options for abort modes (such as return to origin, abort to destination, and station-keeping).

C.10.5.5 Non-Crewed Systems

C.10.5.5.1 When a space flight system is used without crew or passengers aboard and in proximity operations to a crewed vehicle, an abort mode to separate a safe distance from the crewed vehicle is to be provided.

C.10.5.6 Space System

C.10.5.6.1 An extended Space System mission duration increases the probability that some emergencies will arise. This requires that the means be provided to manage these emergencies to successful resolution rather than evacuating at the first indication of system malfunction, crew or passenger illness, or injury. This can be accomplished through resilient core system design, including high degrees of failure tolerance, maintainability, skip cycle logistics stores on orbit, a robust logistics chain, and the provision of emergency medical facilities on board. However, the capability to evacuate and return to Earth is to be provided at all times. For Space Station missions, abort and crew escape requirements are functionally the same. Therefore, the program requires an escape vehicle and/or a safe haven, which provides for safe and timely crew and passenger return.

C.10.5.7 Habitable Surface Systems

C.10.5.7.1 A Habitable Surface System is similar to a Space Station in that it will typically have an extended mission duration, but it differs in that the capability for an immediate crew and passenger return will not always be feasible. Therefore, providing a means of dealing with emergencies is required. In many cases, an immediate evacuation in response to an emergency may not be practical. For these situations, emergency medical and safe haven

capabilities including remote medical treatment are significant elements in the system design.

C.10.5.8 Extravehicular Mobility Unit

C.10.5.8.1 Extravehicular Mobility Units operate in the vicinity of a larger space system. Therefore, the minimum reliability of the Extravehicular Mobility Unit provides for enough reserve capacity to allow the crewmember to safely return to the larger space flight systems. This reliability is allocated over the number of required missions of the Extravehicular Mobility Unit. Extravehicular Mobility Units ought to include crew self rescue devices worn by each Extravehicular Activity crewmember during all periods when there is no vehicle to credibly rescue an inadvertently detached Extravehicular Activity crewmember. This device could be the Simplified Aid for Extravehicular Activity Rescue or an equivalent capability.

| TOC | Preface | Chapter1 | Chapter2 | Chapter3 | AppendixA | AppendixB | AppendixC | ALL |

| NODIS Library | Program Management(8000s) | Search |

**DISTRIBUTION:**
**NODIS**